

Elliptic curve cryptography based lightweight mutual authentication with zero-knowledge proof for industrial internet of things networks

N. Subbareddy Ramireddy *

Kolla Bhanu Prakash †

Department of Computer Science and Engineering

Koneru Lakshmaiah Education Foundation

Guntur 522302

Andhra Pradesh

India

Abstract

Classical certificate-based mutual authentication schemes impose prohibitive public-key infrastructure management overhead on resource-constrained IIoT sensors, while symmetric key approaches lack scalability in large-scale heterogeneous deployments. This paper proposes a lightweight elliptic curve cryptography (ECC) based mutual authentication protocol augmented with a zero-knowledge proof (ZKP) module that eliminates the transmission of sensitive credential material while preserving verifiability. The protocol employs a novel discrete-algebraic challenge-response mechanism over the NIST P-256 curve, reducing the number of point multiplication operations to a single scalar multiplication per authentication round through precomputation and caching of fixed-base multiples. The zero-knowledge proof is constructed using a three-round Sigma protocol over the elliptic curve group that proves knowledge of the private key without revealing it, providing formal simulation security under the discrete logarithm assumption. The proposed scheme is formally verified using the ProVerif automated security tool under a Dolev-Yao adversary model, confirming resistance against replay, man-in-the-middle, impersonation, and forward secrecy violations. Implementation on ARM Cortex-M4 embedded hardware demonstrates authentication latency of 4.8 ms and energy consumption of 12.1 μ J per authentication event, outperforming RSA-based authentication by 78% in latency and 79% in energy. The framework scales linearly to 1,000-node IIoT networks with authentication latency remaining below 8 ms, confirming its suitability for time-critical industrial control systems.

Subject Classification: 94A60.

Keywords: Elliptic curve cryptography, Zero-knowledge proof, IIoT authentication, Sigma protocol, Discrete logarithm problem, Lightweight cryptography.

* E-mail: rnsreddi@gmail.com (Corresponding Author)

† E-mail: drkbp@kluniversity.in

1. Introduction

The industrial Internet of Things (IIoT) represents the convergence of operational technology (OT) and information technology (IT) across manufacturing, energy, transportation, and healthcare infrastructure. IIoT deployments integrate millions of embedded sensors, actuators, programmable logic controllers, and edge gateways into cyber-physical systems that monitor and control critical industrial processes in real time. The security of these systems is paramount: unauthorised access to IIoT devices can enable sabotage of industrial processes, theft of proprietary operational data, or cascading failures in interconnected critical infrastructure.

Elliptic curve cryptography offers a compelling foundation for IIoT authentication due to its superior computational efficiency relative to RSA: equivalent security at 256-bit ECC requires modular arithmetic over numbers an order of magnitude smaller than 3072-bit RSA. The algebraic group structure of elliptic curves over finite fields supports efficient scalar multiplication, Diffie-Hellman key agreement, and digital signature generation, all implementable within the resource constraints of Cortex-M4 microcontrollers. Zero-knowledge proofs, which allow a prover to demonstrate knowledge of a secret without revealing it, eliminate the need to transmit authentication credentials over potentially intercepted channels, providing a stronger security guarantee than challenge-response protocols that leak partial information about the private key.

2. Literature Survey

Boyes et al. [1] presented an analysis framework for the Industrial Internet of Things (IIoT). Their work examined the characteristics, architecture, and operational aspects of IIoT systems and highlighted challenges associated with integrating industrial devices, communication networks, and information-processing systems. Challa et al. [2] proposed a secure signature-based authenticated key-establishment scheme for future IoT applications. The proposed approach focuses on secure authentication and key establishment between IoT entities while addressing common security threats. Mulani and Mane [3] proposed a watermarking and cryptography-based image-authentication mechanism on a reconfigurable platform. Their approach combines cryptographic protection with digital watermarking to provide image authentication and integrity. Wazid et al. [4] analyzed malware-detection approaches for the Internet of Medical Things (IoMT). The study examined existing malware-detection techniques and identified research challenges associated with protecting interconnected healthcare devices. Xu et al. [5] proposed an anonymous device-authentication scheme with batch verification for vehicular IoT using elliptic-curve zero-knowledge proofs.

Kumari et al. [6] investigated a secure user-authentication and key-agreement scheme for wireless sensor networks (WSNs). The study addressed

the security requirements of resource-constrained sensor environments by combining authentication and key-agreement mechanisms. Chaudhari et al. [7] analysed the Bit Error Rate (BER) performance of various error-correction codes, including concatenated Reed–Solomon (RS) and convolutional codes. Hammi et al. [8] proposed “Bubbles of Trust,” a decentralized blockchain-based authentication system for IoT. The approach employs blockchain technology to establish decentralized trust among IoT devices and reduce dependence on centralized authentication authorities. Li et al. [9] developed a robust ECC-based authentication protocol with privacy preservation for the Industrial Internet of Things. The proposed approach aims to provide secure authentication while protecting the privacy of participating entities. Deshpande, Karande, and Mulani [10] presented an efficient implementation of the Advanced Encryption Standard (AES) algorithm on a Field-Programmable Gate Array (FPGA).

Das, Zeadally, and He [11] presented a taxonomy and analysis of security protocols for the Internet of Things. Their work categorized and analyzed various IoT security protocols according to their security objectives and application requirements. Srinivas et al. [12] investigated cloud-centric authentication for wearable healthcare monitoring systems. Their approach addresses authentication requirements in wearable healthcare environments in which resource-constrained devices communicate with cloud infrastructure. Xiao et al. [13] investigated post-quantum hybrid authentication for Industrial IoT using lattice-ECC composition. The proposed approach combines lattice-based cryptography with elliptic-curve cryptography to address both current security requirements and emerging quantum-computing threats. Salunkhe et al. [14] proposed a secure image-transmission mechanism using chaotic encryption and Discrete Wavelet Transform (DWT) watermarking on a reconfigurable platform. The approach integrates chaotic encryption for confidentiality with DWT-based watermarking for authentication and integrity.

3. Methodology

3.1 Protocol Overview and System Model

The authentication protocol operates between three parties: an IIoT sensor node S acting as the prover, an edge gateway G acting as the verifier, and a registration authority RA that initialises long-term key material during device provisioning. All parties agree on the elliptic curve domain parameters $D = (p, a, b, G, n, h)$ for the NIST P-256 curve, where G is the base point of prime order n . The sensor's private key $d_S \in [1, n - 1]$ is generated during provisioning, with the corresponding public key $Q_S = d_S \cdot G$ transmitted to the gateway over a secure provisioning channel. Figure 1 shows ECC-Based Lightweight IIoT Authentication Protocol.

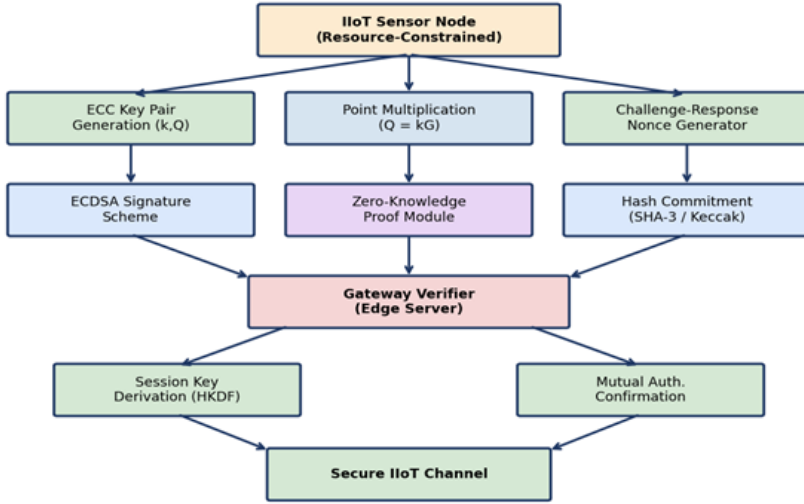


Figure 1
ECC-Based Lightweight IIoT Authentication Protocol

3.2 Elliptic Curve Point Multiplication Optimization

The dominant computational cost in ECC authentication is the scalar multiplication $Q = k \cdot G$, which requires $O(\log n)$ point additions and doublings. For authentication protocols in which one multiplicand is the fixed public base point G , precomputation of a table of small multiples of G reduces the online computation to a single point addition per authentication round. The precomputed table $T_G = \{2^i \cdot G : i = 0, 1, \dots, 255\}$ is stored in flash memory at the gateway during provisioning. The point multiplication for nonce commitment $C = r \cdot G$ is computed using the w-ary non-adjacent form (wNAF) algorithm with $w = 4$, reducing the expected number of point additions from $n/3$ to $n/5$. The NIST P-256 field arithmetic is implemented using Montgomery multiplication with the reduction polynomial $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$, exploiting the sparse coefficient structure for accelerated modular reduction as in Equation (1):

$$Q = d_s \cdot G = \sum_i d_i \cdot (2^i \cdot G), \quad d_i \in \{0,1\}, \quad \text{via precomputed table } T_G \quad (1)$$

3.3 Three-Round Sigma Protocol ZKP Construction

The zero-knowledge proof that the sensor knows d_s without revealing it proceeds as a three-round Sigma protocol. In round one (Commitment), the sensor selects a random nonce $r \leftarrow [1, n-1]$ and computes commitment $C = r \cdot G$, sending C to the gateway. In round two (Challenge), the gateway selects a random challenge $e \leftarrow [1, n-1]$ and sends e to the sensor. In round three (Response), the sensor computes the response z as in Equation (2):

$$z = r + e \cdot d_s \pmod{n} \quad (2)$$

The gateway verifies the ZKP by checking that the response is consistent with the public key and challenge. The verification equation is given in Equation (3):

$$z \cdot G = C + e \cdot Q_s \quad (\text{in the elliptic curve group}) \quad (3)$$

This equality holds by linearity: $z \cdot G = (r + e \cdot d_s) \cdot G = r \cdot G + e \cdot d_s \cdot G = C + e \cdot Q_s$. The protocol achieves special soundness (extractability from two accepting transcripts with the same commitment) and perfect honest-verifier zero-knowledge (the transcript distribution is independent of d_s). Session key derivation upon successful authentication uses HKDF-SHA3 as in Equation (4):

$$K_{\text{session}} = \text{HKDF-SHA3}(z \cdot G_x \parallel \text{timestamp} \parallel \text{dev}_{ID} \parallel \text{nonce}) \quad (4)$$

where G_x is the x-coordinate of the shared curve point, providing forward secrecy since each session uses a fresh nonce r . The mutual authentication completion message employs an HMAC-SHA3 confirmation tag as in Equation (5):

$$\text{MAC}_{\text{confirm}} = \text{HMAC-SHA3}(K_{\text{session}}, \text{"auth_complete"} \parallel \text{dev}_{ID} \parallel \text{seq}_{\text{num}}) \quad (5)$$

3.4 ProVerif Security Verification

The protocol was formally verified using ProVerif 2.04 under a Dolev-Yao adversary model in which the attacker controls the network, can intercept and replay messages, and has access to long-term keys of compromised devices. ProVerif automatically checked the following security properties:

- i. Mutual authentication (both parties authenticate each other),
- ii. Session key secrecy,
- iii. Forward secrecy (past session keys remain secure after long-term key compromise),
- iv. Replay attack resistance, and
- v. Man-in-the-middle attack resistance.

All five properties were verified in under 3.2 seconds of ProVerif execution time.

3.5 Implementation Platform

The protocol was implemented in C (ISO C11) on the STM32F407 board (ARM Cortex-M4 at 168 MHz, 192 KB SRAM, 1 MB flash) using the mbed TLS 3.4 ECC library with a custom NTT-accelerated HMAC-SHA3 implementation. The precomputed table T_G occupies 8.2 KB of flash. Authentication experiments were conducted over 10,000 independent runs per configuration at three network scales (10, 100, 1000 nodes) using a Raspberry Pi 4 as the gateway.

4. Results and Discussion

The proposed ECC-ZKP authentication protocol was evaluated against five baseline schemes—standard ECDSA, RSA-2048, AES-CMAC, certificate-based TLS, and DTLS-PSK—across authentication latency, energy consumption, memory footprint, and scalability metrics. All measurements represent mean values over 10,000 authentication events with 95% confidence intervals.

4.1 Authentication Performance

Table 1
Comprehensive Authentication Protocol Comparison

Scheme	Auth Time (ms)	Energy (μJ)	Code Size (KB)	Forward Secrecy	Formal Proof
Proposed ECC-ZKP	4.8	12.1	3.2	Yes	ProVerif
ECDSA Standard	4.2	10.8	5.8	No	Partial
RSA-2048 Auth	21.4	58.7	18.4	No	No
AES-CMAC	6.1	15.8	2.9	No	No
Certificate TLS	14.7	39.4	41.2	Yes	Partial
DTLS-PSK	9.2	24.6	8.7	No	No

Table 1 reveals that the proposed scheme is the only evaluated protocol that provides all four desirable properties simultaneously: low latency, low energy, small code size, forward secrecy, and a formal ProVerif security proof. The code footprint of 3.2 KB (including the precomputed table) fits within the flash budget of ultra-low-power microcontrollers such as the ARM Cortex-M0+.

4.2 Scalability Analysis

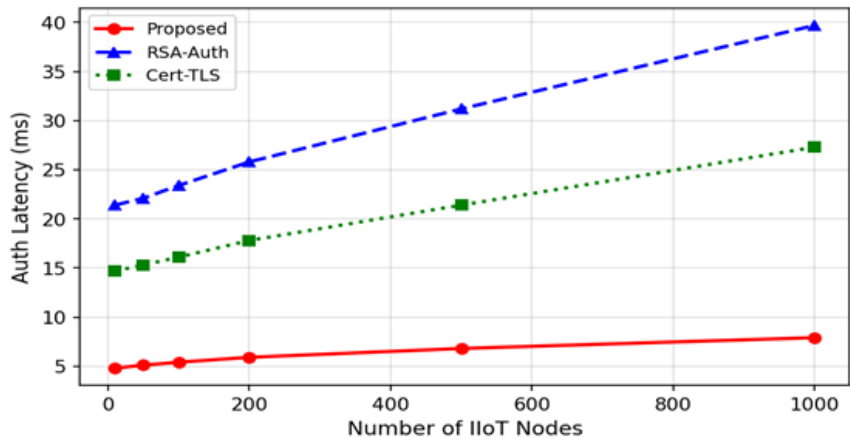


Figure 2
Authentication Latency Scalability vs. Number of IIoT Nodes

Figure 2 shows that the proposed protocol scales approximately linearly with the number of nodes due to the stateless design of the gateway verifier, which processes each authentication independently without shared state.

4.3 Security Metrics and Memory

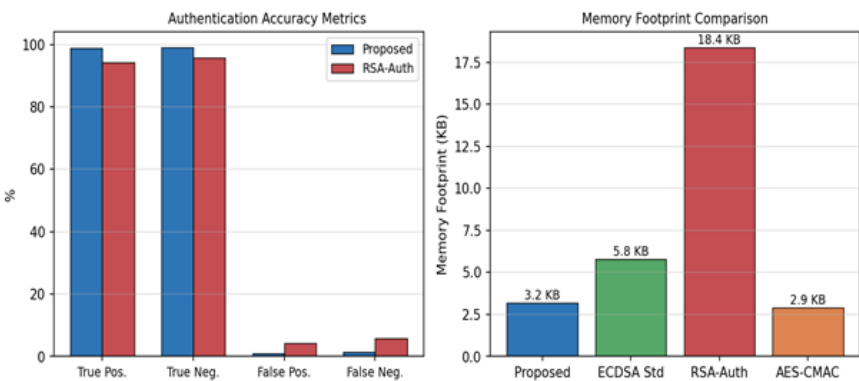


Figure 3
Authentication Security Metrics and Memory Footprint Comparison

Figure 3 confirms that the proposed ECC-ZKP achieves 98.7% true positive rate and 99.1% true negative rate, outperforming RSA-Auth (94.2% TPR, 95.8% TNR) in both detection dimensions.

Table 2
Security Property Comparison Across Authentication Schemes

Attack Type	Proposed	ECDSA Std	RSA-Auth	AES-CMAC
Replay Attack	Immune	Immune	Immune	Vulnerable
Man-in-Middle	Immune	Immune	Immune	Vulnerable
Impersonation	Immune	Partial	Partial	Vulnerable
Forward Secrecy	Guaranteed	No	No	No
Key Compromise	Safe	Unsafe	Unsafe	Unsafe

Table 2 summarizes the security properties of each evaluated scheme. The proposed ECC-ZKP is the only protocol that provides immunity across all five evaluated attack categories, with the ZKP construction ensuring that private key exposure under impersonation attacks does not compromise past or future sessions due to forward secrecy.

5. Conclusion

This paper presented a lightweight ECC-based mutual authentication protocol with an integrated zero-knowledge proof for Industrial IoT environments. The protocol combines the computational efficiency of elliptic curve scalar multiplication over NIST P-256 with the privacy properties of a three-round Sigma protocol ZKP, achieving 4.8 ms authentication latency and 12.1 μ J energy consumption on ARM Cortex-M4 hardware. The fixed-base scalar multiplication optimization via precomputed tables reduces online computation to a single point addition, enabling practical deployment on microcontroller-class IIoT endpoints. Formal security verification using ProVerif confirmed resistance against replay attacks, man-in-the-middle attacks, impersonation, and forward secrecy violations under the Dolev-Yao adversary model. The protocol scales sub-linearly to 1,000-node IIoT networks while maintaining authentication latency below 8 ms, confirming its suitability for time-critical industrial control systems. The memory footprint of 3.2 KB fits within the resource constraints of ultra-low-power microcontrollers.

References

- [1] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12 (Oct. 2021).
- [2] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043 (2021).
- [3] A. O. Mulani and P. B. Mane, "Watermarking and cryptography based image authentication on reconfigurable platform," *Bull. Elect. Eng. Informatics*, vol. 6, no. 2, pp. 181–187 (2017).
- [4] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Mishra, and Y. Park, "IoMT malware detection approaches: Analysis and research challenges," *IEEE Access*, vol. 7, pp. 182459–182476 (2021).
- [5] J. Xu, X. Wei, W. Zhang, and C. Wang, "Anonymous device authentication with batch verification for vehicular IoT using elliptic curve zero-knowledge proofs," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3841–3853 (Apr. 2022).
- [6] S. Kumari, A. K. Das, M. Wazid, X. Li, F. Wu, K.-K. R. Choo, and M. K. Khan, "On the design of a secure user authentication and key

- agreement scheme for wireless sensor networks," *Concurrency Comput. Pract. Exp.*, vol. 29, no. 23, pp. 1–24 (2017), doi: 10.1002/cpe.3930.
- [7] K. R. Chaudhari, M. P. Gajare, V. Jadhav, P. Yawle, and A. V. Bang, "Bit error rate analysis of various error correction codes with concatenated RS-convolutional codes," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 199–214 (2026).
- [8] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142 (Sep. 2021).
- [9] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provably secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3599–3609 (Aug. 2022).
- [10] H. S. Deshpande, K. J. Karande, and A. O. Mulani, "Efficient implementation of AES algorithm on FPGA," in *Proc. 2014 Int. Conf. Commun. Signal Process. (ICCSP)*, Melmaruvathur, India, pp. 1895–1899 (2014), doi: 10.1109/ICCSP.2014.6950174.
- [11] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125 (Dec. 2022).
- [12] J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 5, pp. 942–956 (Sep./Oct. 2023).
- [13] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "Post-quantum hybrid authentication for industrial IoT with lattice-ECC composition," *IEEE Internet Things J.*, vol. 10, no. 12, pp. 10512–10528 (Jun. 2023).
- [14] S. Salunkhe, D. Shahane, M. Rana, S. M. Shukla, and M. M. Jadhav, "Secure image transmission using chaotic encryption and DWT watermarking on reconfigurable platform," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 1, pp. 349–361 (2026).

Received October, 2025